ICS 03.060
CCS A 11

T/SZFCC

苏州市金融业商会团体标准

T/SZFCC XXXX—XXXX

数字人民币2.5层金融机构接入运营机构技术规范

Technical specifications for access of tier 2.5 financial institutions to operational institutions for e-CNY

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

苏州市金融业商会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏金服数字集团有限公司提出。

本文件由苏州市金融业商会归口。

本文件起草单位：江苏金服数字集团有限公司、苏州金服实验室科技有限公司。

本文件主要起草人：

数字人民币 2.5 层金融机构接入运营机构技术规范

1 范围

本文件规定了数字人民币2.5层金融机构接入运营机构的总体原则、网络与防护要求、数据采集与管理要求、2.5层金融机构系统技术要求、接口接入要求、运营管理要求和应急处置等要求。

本文件适用于接入运营机构，通过数字人民币2.5层生态服务平台开展数字人民币业务的各类2.5层金融机构，包括商业银行、村镇银行、支付机构、金融科技公司及其他符合条件的金融类主体。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 17901（所有部分） 信息技术 安全技术 密钥管理

GB/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

运营机构 operating institution

经中国人民银行指定，承担数字人民币发行、回笼、钱包管理、交易处理、资金清算、技术支撑等核心职责的商业银行。

3.2

2.5 层金融机构 tier-2.5 participant financial institution

依托运营机构数字人民币底层能力，通过2.5层生态服务平台，为终端用户提供数字人民币钱包服务、支付结算、场景应用、营销服务、资金监管等服务的金融机构或类金融机构。

3.3

2.5 层生态服务平台 tier-2.5 ecological service platform

依托运营机构底层数字人民币能力搭建的统一服务中台，为商业银行、支付机构、金融科技公司等2.5层金融机构提供标准化接入网关、接口管理、风控调度、合约服务、跨境交互、数据可信存证等公共支撑能力，是连接运营机构与各类2.5层接入主体的中间载体。

4 总体原则

4.1 合规性原则

接入工作应遵守国家相关法律法规、监管政策及数字人民币管理规定，接入机构健全合规、风控和审计体系，落实各类监管要求与合作约定，并主动配合各级监管与运营方开展核查整改，全面防范合规风险。

4.2 安全性原则

搭建覆盖网络、系统、数据、接口、终端、人员和业务的全链路安全防护体系，网络、系统、数据各层面分别落实隔离防护、等级保护测评、加密脱敏等安全举措，全方位保障交易、资金、数据与系统运行安全。

4.3 标准化原则

统一接入全流程、接口、数据、安全四大类标准，明确各环节规范、技术参数与管理要求，平台同步提供全套标准化文档、测试环境及操作手册。

4.4 可控性原则

2.5层生态服务平台对接入机构实行全流程管控，从源头开展资质准入审核，落实分级最小权限管理，对接口调用、流量传输进行限制监控，依托风控机制进行异常预警、拦截与处置。

4.5 兼容性原则

全面适配数字人民币底层各项功能，覆盖线上、线下各类业务场景和多类终端设备以及不同类型接入机构，同时支持接口版本迭代与系统平滑升级，顺应技术、政策及业务变化持续稳定运行。

4.6 可扩展性原则

整体采用微服务、分布式架构，系统、接口、数据模型、功能模块及接入生态均预留扩展空间，支持资源扩容、版本迭代、数据拓展、功能新增与接入主体扩容，灵活适配业务增长、需求创新与生态规模化发展的长期要求。

5 网络与防护要求

5.1 网络架构

5.1.1 网络分区

5.1.1.1 2.5 层金融机构应划分独立的数字人民币业务域，与办公网、互联网、其他业务网进行物理隔离或逻辑隔离，业务数据跨域不应随意流转。

5.1.1.2 网络架构采用分层设计，分为接入层、传输层、核心层，各层级部署防火墙、入侵检测、流量监控等设备。

5.1.1.3 接入网络应支持专线、VPN 等安全传输方式，保障运营机构与金融机构间数据传输的保密性、完整性、真实性。

5.1.1.4 网络带宽应满足业务并发需求，结合交易规模、API 调用频次、数据传输量合理规划带宽，预留冗余带宽。

5.1.1.5 网络设备应选用符合国家信息安全标准的合规设备，定期进行固件升级、配置加固，关闭不必要端口与服务，减少安全暴露面。

5.1.2 网络隔离

5.1.2.1 数字人民币业务网与办公网、互联网与其他业务网之间应采用物理隔离或高强度逻辑隔离方式，内容如下：

a) 域间访问最小权限管控，仅放行经审批的 IP、端口、协议；
b) 跨域传输全程加密、签名、全量审计；
c) 定期开展漏洞扫描、渗透测试，验证隔离策略有效性。

5.1.2.2 应部署下一代防火墙、入侵防御系统、网闸设备和安全隔离网关，配置访问控制列表（ACL）、白名单策略、端口过滤规则、协议过滤规则、应用过滤规则，允许指定 IP、指定端口、指定协议、指定应用进行跨网通信，所有跨网数据传输均宜加密、签名、审计。

5.1.2.3 数字人民币业务域内各子区域之间采用子网隔离、VLAN 划分、防火墙隔离、ACL 控制，每个子区域独立划分网段、独立配置 VLAN、部署安全设备和制定防护策略。

5.1.2.4 跨机构网络连接应采用专线、加密 VPN、国密加密隧道，不应通过互联网直接建立连接，跨机构通信链路全程加密、签名、认证和审计，双方网络出口 IP、端口、协议实行白名单管控，防范跨机构网络攻击、数据窃取、流量劫持风险。

5.1.2.5 网络隔离应定期开展合规检查、安全审计、漏洞扫描和渗透测试，核查隔离策略有效性、隔离设备安全性、跨网通信合规性，及时发现并整改隔离漏洞、策略失效、违规连通等问题，定期更新白名单、访问控制策略、过滤规则。

5.1.3 接入链路

5.1.3.1　2.5层金融机构接入运营机构和2.5层生态服务平台，应采用专线、IPsec VPN、国密加密隧道三种安全链路方式之一，不应通过互联网直接传输数字人民币交易数据、用户敏感信息、业务核心数据，所有接入链路应全程加密、签名、认证、审计。
5.1.3.2　接入链路带宽应满足业务峰值并发需求，应对业务增长、促销活动、突发流量等场景，避免带宽不足导致交易延迟、超时、失败，保障数字人民币交易实时性、高效性、稳定性。
5.1.3.3　关键接入链路采用双链路冗余部署，主链路故障时自动切换至备用链路，无数据丢失、交易中断、业务异常，避免单点故障导致数字人民币业务全面中断，保障业务高可用、高可靠、高连续运行。
5.1.3.4　接入链路应选用运营商骨干专线、优质VPN服务，定期开展链路质量监测、带宽利用率分析、稳定性测试，及时排查链路故障、带宽瓶颈和质量下降等问题，优化链路配置、调整带宽资源、更换故障链路。
5.1.3.5　接入链路应建立常态化运维监控机制，实时监控链路连通性、带宽利用率、延迟、丢包率、流量异常、连接异常等指标，设置分级预警阈值，对异常情况及时告警、快速排查、高效处置；定期开展链路应急演练、故障切换演练，提升链路故障应急处置能力，保障接入链路故障时快速恢复、业务平稳过渡。

5.1.4　网络拓扑

5.1.4.1　业务网络应具备分层管控、无单点故障、易于运维扩展的高可用网络架构能力，满足流量分级管控、故障快速切换、地址规范可追溯要求。
5.1.4.2　网络拓扑遵循扁平化、高可用原则，简化层级与路由；核心设备双机热备、链路冗余，关键节点无单点故障，保障网络稳定、易运维、高容错。
5.1.4.3　统一规划IP、子网、VLAN 及端口，采用私网地址避免冲突；按业务域划分网段与VLAN，配置标准化、文档化、可追溯。
5.1.4.4　严控节点、设备、链路数量，避免拓扑臃肿；及时清理非必要节点与闲置链路，保持网络简洁可控。
5.1.4.5　网络具备良好扩展性，核心与汇聚层预留设备、端口、带宽资源；地址与VLAN规划留足扩展空间，适配业务增长与场景迭代需求。

5.1.5　网络地址与端口

5.1.5.1　数字人民币业务网统一规划私网 IP，不应公网 IP 承载核心业务；按业务域划分子网，地址分配文档化、标准化、可追溯。
5.1.5.2　网络端口遵循最小开放原则，仅开放业务宜端口与协议，关闭非必要及高危端口，防范端口暴露引发的网络攻击与入侵风险。
5.1.5.3　核心组件不直接暴露公网IP与端口；对外服务经防火墙、WAF、网关做映射与过滤，仅放行指定端口、协议与IP，避免公网直连。
5.1.5.4　定期开展端口合规检查、审计与扫描，清理闲置、高危、违规端口，更新过滤规则与白名单，防范端口扫描与攻击风险。
5.1.5.5　IP与端口配置实行变更审批管理，分配、变更、映射应审批留痕并同步安全策略，不应私自修改网络配置，确保全程合规可追溯。

5.2　网络安全防护

5.2.1　等级保护

5.2.1.1　机构数字人民币业务系统应通过网络安全等级保护三级测评，覆盖网络、主机、应用、数据、接口、终端、管理全维度，应遵循GB/T 22239标准，由具备国家资质的机构测评，确保结果权威合规。
5.2.1.2　等级保护三级每年至少复测一次；系统重大变更或发生安全事件后应专项复测。发现漏洞与隐患应限期整改、闭环管理，持续符合三级要求。
5.2.1.3　成立等级保护专项工作组，明确责任分工，统筹备案、测评、整改、运维全流程；建立等级保护、安全、运维、应急管理制度，保障工作常态化、规范化、制度化。

5.2.1.4　测评重点覆盖网络、主机、应用、数据、接口、终端、人员、管理、风控、审计、应急安全，核查隔离、访问控制、加密脱敏、漏洞防护、日志审计、权限管控等关键措施落实情况，确保全面无遗漏。

5.2.1.5　等级保护相关文档应完整归档、专人管理、定期备份，留存不低于 5 年；应保密、防泄漏篡改，满足监管、审计、追溯、复盘要求。

5.2.2　边界防护

5.2.2.1　数字人民币业务网网络边界应部署下一代防火墙、入侵检测系统、入侵防御系统、抗 DDoS 设备、Web 应用防火墙，构建多层防护体系，全面防范跨网攻击、入侵、劫持、窃取、拒绝服务等风险。

5.2.2.2　下一代防火墙应配置访问控制策略、白名单策略、端口过滤规则、协议过滤规则、应用过滤规则、流量控制策略、NAT 策略，实时监控边界流量，拦截非法访问、越权访问、违规流量、恶意连接，阻断非授权通信、高危协议、恶意应用。

5.2.2.3　入侵检测系统（IDS）、入侵防御系统（IPS）应实时监测边界网络流量、网络行为、系统日志、接口调用日志，识别并拦截 SQL 注入、XSS 跨站脚本等各类网络攻击与恶意行为，实时告警、快速阻断、溯源核查。

5.2.2.4　抗 DDoS 设备应部署在互联网边界、跨机构链路边界，实时监测边界流量，通过流量清洗、带宽扩容、流量调度、攻击识别、异常拦截等技术手段，保障业务系统在大流量攻击下稳定运行、业务不中断、数据不丢失。

5.2.3　访问控制

5.2.3.1　建立网络访问控制，采用 IP、端口、应用三重白名单，仅允许指定 IP、端口、应用接入，非白名单访问一律拦截告警，从源头防范非法接入。

5.2.3.2　遵循最小权限、按需开放、定期清理原则，严控权限与端口开放；定期更新白名单与策略，清理闲置 IP、无效端口与过期权限，确保访问精准可控。

5.2.3.3　采用身份认证、权限分级、访问审计、行为监控多重手段，所有访问与操作应核验身份与权限，权限隔离分级，全程可追溯，防范越权与滥用。

5.2.3.4　访问控制覆盖网络、主机、应用、接口、数据全层级，各层分别通过防火墙、权限管控、密钥校验、数据脱敏等措施。

5.2.3.5　建立常态化监控审计机制，实时监测访问行为并设置预警阈值，异常及时告警处置；定期开展合规审计与策略评估，整改访问控制漏洞。

5.2.4　传输加密

5.2.4.1　数字人民币业务网内外所有数据传输，采用 TLS 1.3+国密 SM4 双重加密，密钥轮换符合 GB/T 17901（所有部分）要求。

5.2.4.2　数据传输签名采用 SM2+SM3，接口、交易、配置数据均带签名；接收方验签，防篡改、重放、伪造，确保真实、完整、不可抵赖。

5.2.4.3　密钥轮换周期应按照国家密码主管部门规定及密钥使用风险等级确定，符合 GB/T 17901（所有部分）的要求。

5.2.4.4　定期检查加密合规、算法有效性与密钥安全，升级老旧协议、淘汰弱算法、修复漏洞；开展加密测试与渗透测试，防范破解、攻击与泄漏风险。

5.2.5　日志审计

5.2.5.1　数字人民币业务网所有设备与系统均开启全量日志，覆盖网络、访问、交易、配置、告警、运维等全活动，全程留痕、可追溯审计。

5.2.5.2　日志审计常态化智能化，实时监控异常并分级告警处置；定期审计排查风险，发现隐患及时整改闭环。

5.2.5.3　日志管理应保密合规，仅授权人员访问；导出、共享、销毁应审批留痕并加密处理。

6　数据采集与管理要求

6.1 数据分类

6.1.1 核心敏感数据

6.1.1.1 核心敏感数据涵盖个人及企业高隐私资金信息，应实施最高等级防护与加密存储管控；数据仅用于核心业务流程，应遵循最小必要原则，不应外溢共享与营销使用。
6.1.1.2 数据全链路应国密加密脱敏、分级双人管控、独立隔离存储，并常态化开展安全审计与风险检测。

6.1.2 业务数据

6.1.2.1 业务数据包含商户、订单、交易流水、营销、接口日志及系统配置等信息，用于业务运营、结算风控与运营优化，采集应真实合规、经标准化校验清洗保证数据质量。
6.1.2.2 业务数据应在合作机构间经审批、加密、留痕后按需共享，不应外泄滥用，并建立常态化监控审计机制，及时处置数据安全与质量异常。

6.1.3 公开数据

公开数据应包含机构脱敏资质、产品场景、公开接口文档、接入流程、公告协议等对外公示类材料，可供公众查阅传播；发布前应完成合规审核，剔除敏感涉密、虚假违规内容，使用者标注来源、不应篡改数据或擅自商用，平台对其享有知识产权，同时建立公开数据发布、更新、归档、定期核查整改的全生命周期管理机制。

6.2 数据采集

6.2.1 采集范围

6.2.1.1 企业用户数据含证件类型、名称、信用代码、有效期、联系方式、法人信息、营业执照等，应真实完整、加盖公章。
6.2.1.2 个人用户数据含姓名、手机号、身份证号、钱包信息、注册与设备信息；敏感信息脱敏存储，仅限核验风控追溯。
6.2.1.3 交易数据含流水、时间、金额、钱包 ID、订单号、商户号、状态、对账结算退款撤销标识等，覆盖全流程，可追溯对账审计风控。
6.2.1.4 接入数据含机构 ID、Appid、接口信息、调用日志、IP 设备、状态、限流熔断、签名加密等，覆盖调用全链路，可管控监控审计追溯。
6.2.1.5 风控合规数据含用户行为、交易风险、异常操作、合规审核、反洗钱、资质权限、日志审计、安全事件记录，支撑风控核查处置复盘。

6.2.2 采集授权

6.2.2.1 个人信息采集应经用户明示同意，清晰告知采集目的、用途、存储期限与保护措施，不应强制、默认、隐瞒或欺骗授权。
6.2.2.2 企业信息采集应经法人授权并加盖公章，提交授权委托书与资质文件，明确数据用途；未成年人信息采集应获得监护人明示同意并核验身份，保护未成年人权益。
6.2.2.3 采集授权全程留痕、加密存储、长期留存，支持追溯审计；用户/企业可随时撤回授权、查询、更正、删除信息，平台提供便捷渠道及时响应。

6.3 数据存储

6.3.1 加密存储

6.3.1.1 核心敏感数据采用国密 SM4 加密存储，密钥与数据物理分离、专人保管、定期轮换，不应明文存储与泄露，保障敏感数据安全。
6.3.1.2 业务数据采用 AES-256 或 SM4 加密存储，密钥分级管理、定期更新；存储环节全程加密，防止数据泄露、篡改、丢失与滥用。
6.3.1.3 密钥管理遵循国密标准，全程留痕、双人双岗、定期轮换；定期开展加密合规审计与安全测试，及时整改漏洞，保障数据存储安全可控。

6.3.2 数据脱敏

6.3.2.1 前端、日志、报表、接口返回、测试环境中，核心敏感数据应脱敏，手机号、身份证号、钱包 ID、姓名等按统一规则处理。
6.3.2.2 各类日志不应留存明文敏感数据，手机号、身份证号、钱包 ID、余额、交易明细等均宜脱敏记录。
6.3.2.3 报表、文件、备份导出敏感数据一律脱敏，导出文件加密管控、专人管理，防止数据泄露、滥用与流失。
6.3.2.4 接口返回、测试、联调、沙箱数据宜脱敏处理，测试环境不应使用真实未脱敏敏感数据，保障测试数据安全合规。
6.3.2.5 制定统一脱敏规则并定期审核优化，覆盖全场景；定期开展合规检查与漏洞排查，确保脱敏持续有效、敏感信息不泄露。

6.3.3 存储期限

6.3.3.1 交易数据、风控数据、合规数据的留存期限不应少于 5 年，日志数据留存期限不应少于 6 个月。
6.3.3.2 用户注册、资质、实名、钱包等基础数据，留存至用户注销、企业退出后继续保存，到期不可逆销毁敏感信息、留存匿名审计数据。
6.3.3.3 应按法规监管执行存储期限，建立生命周期管理，定期清理过期冗余数据，保障合规高效安全可控。

6.4 数据共享与流转

6.4.1 共享范围

6.4.1.1 数据共享仅限运营机构、生态平台、接入金融机构三方，用于数字人民币业务、风控、合规、对账与运维。
6.4.1.2 机构间共享应审批、按需最小范围开放，仅共享非敏感脱敏数据，不应共享敏感信息与核心数据；共享宜签订保密协议、加密传输、全程留痕。
6.4.1.3 数据共享仅限合规业务、风控、运营优化与场景落地，不应用于商业营销、数据交易、违规获利等用途。
6.4.1.4 监管或司法部门依法调证时，核验法定文书并经合规审批后提供数据，全程留痕审计，配合监管同时保障数据安全与隐私。
6.4.1.5 应建立全流程管理机制，定期核查合规性，清理违规无效共享。

6.4.2 流转管控

6.4.2.1 数据流转全程加密签名、认证审计，传输交换采用 TLS1.3+SM4 加密、SM2/SM3 签名及身份校验。
6.4.2.2 流转实行分级权限、按需最小范围开放，仅授权主体可操作，仅流转必要数据；全程留痕，记录完整信息，可追溯审计。
6.4.2.3 重要及敏感数据流转宜合规审批、双人复核、加密严控，流转前后核查监控、归档审计。
6.4.2.4 不应随意跨网跨境流转，核心数据不应跨境传输；跨境应经监管审批、加密监控，符合相关法规要求。
6.4.2.5 建立常态化流转监控审计机制，实时识别异常风险并及时处置整改，保障流转全程合规安全可控可追溯。

6.4.3 跨境限制

6.4.3.1 应遵循数据跨境相关法规要求，数字人民币全量数据未经审批不应跨境流转，从源头防范跨境安全风险。
6.4.3.2 个人及企业核心敏感数据、交易、风控、合规涉密数据，一律不应跨境传输、存储与共享。
6.4.3.3 确有必要跨境传输非敏感数据的，应完成安全评估与审批，使用合规通道并全程加密监控；同时建立全流程专项管理机制，定期排查整改风险。

6.5 数据销毁

6.5.1 销毁场景

6.5.1.1 个人用户注销账号、撤回授权或申请删除信息时，立即销毁其敏感及冗余数据，仅留存匿名审计数据。
6.5.1.2 企业用户终止业务、合作结束或资质失效后，销毁敏感、冗余及非必要资质材料，保留合规追溯数据。
6.5.1.3 数据存储期限届满、过期数据、冗余数据、无效数据、测试数据、联调数据、沙箱数据、临时数据、中间数据、备份冗余数据，达到清理、销毁条件时，定期触发数据销毁流程，不可逆销毁过期、冗余、无效数据，释放存储资源。
6.5.1.4 涉及的风险数据、异常数据、可疑数据、违规数据，需立即触发数据销毁流程，不可逆销毁风险数据，消除安全隐患，不应风险扩散、泄漏扩大、损失加剧。
6.5.1.5 法律法规、监管政策、行业规范、平台制度更新，要求销毁特定数据、清理特定信息、删除特定内容时，按规定立即触发数据销毁流程，不可逆销毁相关数据。

6.5.2 销毁方式

6.5.2.1 核心敏感数据销毁，采用磁盘物理销毁、数据覆写、数据库硬删除、备份同步销毁、文件粉碎等不可逆方式，确保数据彻底删除、无法恢复、不可还原，杜绝数据残留、恢复泄漏风险。
6.5.2.2 业务数据、日志数据、测试数据、临时数据等非核心敏感数据销毁，采用数据库硬删除、文件粉碎、格式化销毁、备份同步清理、数据碎片清理、索引删除、缓存清空等不可逆方式，同时清理相关索引、缓存、备份、冗余数据，不应数据残留、泄漏。
6.5.2.3 加密数据销毁，同时销毁数据本体、加密密钥、密钥备份、加密配置、解密工具、密钥缓存，从数据和密钥两端彻底销毁，杜绝加密数据被解密恢复、泄漏滥用风险。
6.5.2.4 电子文档、扫描件、资质材料、报表文件、导出文件、备份文件等文件类数据销毁，采用文件粉碎、磁盘格式化、物理销毁存储介质、云存储文件永久删除、备份同步销毁、碎片清理等不可逆方式。
6.5.2.5 数据销毁后留存销毁记录、销毁时间、销毁方式、销毁内容、销毁执行人、复核人、销毁结果、校验记录，销毁记录加密存储、长期留存、可追溯、可审计。

6.5.3 销毁校验

6.5.3.1 数据销毁后通过多种方式全面校验，确保数据彻底删除、无法恢复，校验不通过宜重新销毁。
6.5.3.2 校验执行双人双岗、交叉复核，全程留痕并签字确认。核心敏感数据额外开展恢复、解密等专项测试，确认数据完全清除。
6.5.3.3 核心敏感数据销毁校验，额外开展数据恢复测试、密钥解密测试、磁盘碎片分析、备份恢复校验，尝试通过专业恢复工具、解密工具、备份恢复手段恢复销毁数据，确认无法恢复、信息不可读取、数据彻底清除。
6.5.3.4 完整留存销毁校验台账，加密长期保存，满足审计追溯需求；规范数据销毁全流程管理，定期核查评估，整改各类问题，保障销毁合规彻底。

7 2.5 层金融机构系统技术要求

7.1 系统架构

7.1.1 分层架构

7.1.1.1 2.5 层金融机构数字人民币业务系统宜采用五层分层架构，分为前台展业层、场景应用层、业务应用层、能力服务层、数据管理层，模块独立部署、互不干扰，支持独立扩容、升级、降级、熔断，适配业务快速迭代与扩展需求。
7.1.1.2 系统应具备分层解耦、模块独立迭代、故障隔离的业务分层能力，支持各业务模块独立扩容、降级、灰度更新，适配多场景灵活部署。

7.1.1.3 前台展业层面向终端用户，提供 PC 管理端、H5 端、APP 端、安卓终端、iOS 终端等多终端访问入口；系统应支持苏惠青年卡、文旅硬钱包、外币兑换机配套硬钱包的开卡、充值、离线交易对账能力，覆盖苏州线下海量受理终端。

7.1.1.4 场景应用层应聚焦业务场景落地，整合电商购物、供应链金融、线下商超、售卖机等多元场景能力，单独增设多边货币桥跨境业务模块，匹配苏 2.5 层银行跨境汇款、跨境缴税业务需求，提供定制化配置，细化跨境贸易完整服务技术标准，内容如下：

a) 保税仓储数据交互：统一出入库单、货权凭证、库存、物流报文标准，采用 TLS1.3+SM4 传输、SM2/SM3 验签；支持实时增量、日终批量同步，涵盖企业、报关、商品、货权等关键字段；

b) 跨境合规服务节点交互：对接海关、跨境征信、外汇合规服务商，统一主体资质、贸易单据、资金流水交互接口；合规校验结果实时回传，自动拦截高风险业务并留存记录。

7.1.1.5 业务应用层承担核心业务流程处理，涵盖用户注册、资质审批、商户进件、钱包管理等核心业务功能，负责业务逻辑实现、流程流转、规则执行、数据交互、权限管控。

7.1.1.6 能力服务层封装底层核心技术能力，包括钱包管理服务、支付结算服务、API 接入服务、风控引擎服务和智能合约服务等，应集成苏州统一智能合约网关，支持预付资金监管、跨境税费自动扣划、企业薪资批量代发合约模板。

7.1.1.7 数据管理层负责全量数据的存储、管理、治理、分析和安全防护，涵盖用户数据、钱包数据、交易数据、跨境贸易单据、商业实体基础信息、项目级合规档案（KYC、财务审计材料）等，提供数据安全相关的防护能力。

7.1.1.8 针对村镇银行、小型支付机构等规模较小、业务场景单一的 2.5 层金融机构，可结合自身业务体量、客户规模、运营场景采用简化分层架构，允许合并层级、精简模块，宜完整覆盖钱包管理、支付结算、风控、数据安全、接口接入等核心业务能力。

7.1.2 微服务设计

7.1.2.1 系统整体采用微服务架构，将钱包管理、支付结算、API 接入、风控引擎、智能合约、用户管理、商户管理等核心功能拆分为独立微服务，每个微服务专注单一业务能力、独立开发、独立部署、独立运维和独立扩容。

7.1.2.2 微服务之间通过 RESTful API、RPC、消息队列进行通信，接口标准化、协议统一、格式规范、版本可控，支持同步调用、异步解耦、流量削峰、故障隔离。

7.1.2.3 每个微服务具备独立数据库、独立缓存、独立配置、独立日志、独立监控、独立告警，数据隔离、资源隔离、权限隔离、故障隔离，避免数据相互干扰、资源争抢、故障扩散，支持微服务独立升级、独立回滚、独立扩容、独立降级，适配业务模块快速迭代、功能独立更新需求。

7.1.2.4 微服务应具备模块解耦、独立迭代、故障隔离、弹性扩缩容的分布式服务能力，满足以下硬性能力要求：

a) 业务功能模块化拆分，单一模块故障不扩散至全系统；

b) 支持独立扩容、独立升级、版本回滚，不中断整体业务；

c) 配套服务注册发现、流量管控、链路追踪、监控告警基础管控能力；

d) 支持同步/异步通信、流量削峰，适配交易峰值压力。

7.1.2.5 微服务架构应具备服务注册、服务发现、配置中心、网关路由、熔断降级、限流风控、链路追踪、监控告警、日志聚合等基础组件，统一管理微服务生命周期、配置、路由、流量、依赖、监控、日志，简化运维复杂度、提升运维效率、保障微服务集群稳定可靠、高效运行。

7.1.3 高可用设计

7.1.3.1 系统核心组件应双机热备、集群部署、冗余配置、无单点故障，核心节点、核心链路、核心设备均采用冗余设计。

7.1.3.2 数据库采用主从复制、读写分离、分库分表、集群部署，主库负责写入、从库负责查询，提升数据库读写性能、并发处理能力，在主库故障时自动切换至从库，保障数据读写不中断、数据一致、无丢失；大数据量场景下分库分表，分散存储压力、提升查询效率、保障数据库稳定运行。

7.1.3.3 缓存采用分布式缓存集群、多副本存储、数据持久化、故障转移，缓存数据多副本存储、节点冗余、数据持久化，避免缓存节点故障导致数据丢失、缓存击穿、缓存雪崩。

7.1.3.4 应用服务采用集群部署、负载均衡、弹性伸缩、灰度发布、蓝绿部署，多节点集群部署、负载均衡分发流量，避免单节点压力过大、性能瓶颈、故障影响全局；弹性伸缩应对流量峰值，灰度发布、蓝绿部署保障版本平滑升级、无业务中断、故障可快速回滚。
7.1.3.5 网络与链路采用双链路冗余、多运营商接入、专线冗余、设备双机热备，核心网络设备、接入链路、专线均冗余配置，避免网络单点故障、链路中断、运营商故障导致业务中断，保障网络连通性、稳定性、可靠性、高可用，支撑业务持续稳定运行。

7.2 核心功能能力

7.2.1 钱包管理

7.2.1.1 对公钱包具备开户、转账、资金归集、账户管控、对账风控等完整功能，个人钱包支持开户、收付、实名、设备管理、安全校验等功能，适配日常消费、转账等使用需求。
7.2.1.2 钱包生命周期管理覆盖注册、实名认证、开通、使用、变更、冻结、解冻、注销、销户全流程，执行资质核验、身份认证、权限管控、风控审核、合规追溯。
7.2.1.3 钱包安全管控支持交易密码、短信验证码等多重安全机制，全方位防范密码泄露、账户被盗、资金盗刷、交易篡改、异常操作、权限滥用等安全风险。
7.2.1.4 钱包对账与风控支持支持多形式对账及全维度风控监测，及时处置异常，确保账实相符、风险可控。

7.2.2 商户进件

7.2.2.1 商户注册主体覆盖企业、个体工商户、事业单位、政府机构、公益组织、物联网设备主体、内部项目主体等多元类型，基础商业实体模型留存名称、统一社会信用代码、联系方式、经营地址等基础身份字段。
7.2.2.2 统一归集至项目级管理模块分层管控，将 KYC 身份核验属性、财务审计材料、反洗钱合规台账、风险评级等全量合规字段从商业实体基础模型剥离，具体内容如下：

a) 外部销售商户场景：绑定商户经营项目，挂载经营类 KYC、营收审计、交易风控合规字段；
b) 内部专项项目、政务备案场景：挂载政务审批文件、专项资金审计、政务主体专项 KYC 材料；
c) 物联网设备终端场景：挂载设备入网备案、设备主体合规核验、终端交易风控专项字段。

7.2.2.3 资质审核分为初审、复审、终审三级审核，区分实体基础信息核验、项目级合规材料双线审核流程，同步校验主体真实性与对应项目合规资料。
7.2.2.4 商户审核通过后，平台统一分配商户号、接口密钥、测试账号，并配置权限、交易限额、费率、结算、风控、对账等基础规则。同时支持商户动态更新资质、调整参数、切换账户状态及注销操作，配置灵活，适配各类业务需求。
7.2.2.5 平台应提供一站式商户运营服务，覆盖账户、资质、接口、订单、交易、对账、退款、营销及数据报表、日志查询、异常处置等功能，配套咨询反馈、培训指导、上线与运维保障。
7.2.2.6 平台应搭建商户风控合规体系，实时监测交易、资金、接口操作等行为，识别各类异常交易及洗钱、诈骗等风险，通过分级预警、自动拦截、人工复核等方式处置风险。

7.2.3 支付结算

7.2.3.1 主扫支付适配多终端、多场景扫码交易，支持软硬钱包付款，具备实时交易、即时结算、分润、退款、风控及交易追溯等能力，支付高效安全。
7.2.3.2 被扫支付依托各类收银设备完成收款，付款码具备安全防护能力，适配线下各类消费场景，支持实时结算、对账风控与终端管理，收银便捷稳妥。
7.2.3.3 批量转账提供多种数据提交方式，适配薪资发放、资金归集、分账等业务，内置多重校验与风控，可处理异常并留存记录，提升资金处理效率。
7.2.3.4 对账结算支持多种周期与方式的对账、结算操作，可处理账实差异、结算异常，留存日志并支持报表导出，确保账目与资金准确合规。
7.2.3.5 退款撤销支持全额、部分退款及各类交易撤销，执行风控审核与异常拦截，全程留痕可追溯，保障资金返还正常、交易风险可控。

7.2.4 营销活动

7.2.4.1 支持各类营销活动创建、启停与批量管理，可配置规则、预算及风控参数，同步开展数据统计与效果分析，活动配置灵活、合规可量化。
7.2.4.2 涵盖多种红包类型，可按多维度定向投放，支持参数配置与全流程记录、风控监测，发放精准高效、全程可追溯。
7.2.4.3 发放各类补贴并完成多种券类全生命周期管理，灵活设置使用规则与预算，实时核销、动态监控，严控成本与风险。
7.2.4.4 进行各类权益、积分的发放、使用与兑换管理，配套规则配置、数据统计及风控能力，提升用户黏性，运营合规可控。
7.2.4.5 搭建营销风控体系，全流程监测并拦截刷取、套现、作弊等违规行为，严守各项合规要求，定期排查审计，保障活动安全规范运行。

7.2.5 资金监管

7.2.5.1 开立并管理各类监管资金专户，支持账户全生命周期操作与资金管控、流向追踪，确保资金专款专用、风险可控。
7.2.5.2 应针对各类资金执行冻结、解冻操作，区分多种解冻方式并审核校验，冻结资金限制动用，保障资金履约安全。
7.2.5.3 应提供多样化资金归集、分账功能，可灵活配置规则，适配多类业务场景，提升资金管理效率，分配合规可追溯。
7.2.5.4 应落实专款专用要求，划定资金使用范围，实时监控资金全流程动态，及时识别并处置挪用、洗钱等风险，严守监管规范。
7.2.5.5 应支持多类型资金清算与履约管理，依托智能合约进行自动化履约操作，数据不可篡改、全程留痕，保障履约高效合规。

7.2.6 数据可信与合规增值服务

7.2.6.1 内置数据分级授权分发引擎，自动区分核心敏感数据、业务数据、公开数据，仅向合作机构开放业务必需脱敏字段。
7.2.6.2 覆盖商户进件、订单支付、资金监管、供应链履约数字化存证，整合国密签名、区块链存证能力，业务单据、交易流水、合规核验记录、财务审计材料生成不可篡改可信凭证，支持企业、监管、合作机构授权溯源核验。
7.2.6.3 内置自动化合规台账、KYC 档案统一管理、交易反洗钱筛查、跨境业务合规校验工具，自动归集项目级 KYC、财务审计、资质档案，一键生成监管报送、内部审计标准化报表，完整留存全流程操作日志。
7.2.6.4 面向保税仓储、跨境合规服务商、政务平台、物联网终端等外部节点提供标准化可信数据交互通道，统一加密传输、签名验签、访问白名单管控；数据交互按需授权、限时有效，杜绝超范围、无授权数据流转，兼顾多场景数据互通与合规底线。
7.2.6.5 打通钱包、支付、资金监管、智能合约链路，进行交易、履约、资产、合规数据一体化联动；依托分布式可信架构，进行多方主体数据隔离、可控共享，让平台承载交易撮合、资金清算、履约存证、合规核验多重信任职能。

8 接口接入要求

8.1 接入流程

8.1.1 注册申请

8.1.1.1 2.5 层金融机构接入应首先在 2.5 层生态服务平台提交注册申请，信息真实、完整、准确、合规，无虚假填报、错误信息、遗漏内容、违规表述，保障接入主体合法、资质齐全、信息真实、风险可控。
8.1.1.2 注册申请上传全套资质材料，所有材料清晰、完整、真实、有效、加盖公章，确保资质合法、合规、有效、无过期、无伪造、无篡改、无违规记录。

8.1.1.3　注册申请提交后进入初审，核查信息、材料及资质合规性。初审通过进入复审；未通过将注明原因并指引补正，可重新提交审核。
8.1.1.4　注册全流程操作与审核记录完整留存、加密存储，长期可查可审计，满足合规、追溯及风险核查需求。
8.1.1.5　注册通过后，平台分配机构 ID 与测试账号、开通基础权限，并告知后续审核、联调、上线等流程，保障接入有序推进。

8.1.2　资质审核

8.1.2.1　实行初审、复审、终审三级审核，逐级核验资料、主体资质、综合条件，全程留痕可审计，严把准入关口。
8.1.2.2　重点核验机构合法资质、技术风控运维能力，以及经营场景的真实性与合规性，全面排查各类风险。
8.1.2.3　及时同步审核结果，通过则分配相关账号与权限；驳回则列明问题并允许整改重提，所有记录长期留存备查。

8.1.3　申请洽谈

8.1.3.1　对接各条线负责人，敲定合作范围、结算、风控、权责、退出机制等内容，签订合作、保密及合规相关协议。
8.1.3.2　按业务需求按需分配接口权限，严守最小授权原则；明确接口规范、加密规则、联调标准、运维及故障处置要求。
8.1.3.3　落实反洗钱、数据安全等合规要求，确定监控预警、风险处置、审计追责等规则，进行全流程风险管控。
8.1.3.4　整理洽谈纪要、方案及计划并存档，完成接口、密钥、测试环境配置，正式进入联调测试阶段。

8.1.4　联调测试

8.1.4.1　联调测试在专属测试环境进行，机构使用分配的账号、密钥及沙箱数据，完成连通性、功能、压力、安全等多类测试，保障系统稳定安全、运行无误。
8.1.4.2　接口测试核验协议、加密、权限等，确保通信正常；功能测试覆盖全业务流程，模拟各类场景验证功能与数据无误；压力及安全测试针对高并发、攻击风险开展检测，筑牢性能与安全防线。
8.1.4.3　全程留存各类测试资料与记录，测试通过即可提交上线申请；存在问题则整改复测，全部达标后方可进入投产阶段。

8.1.5　上线投产

8.1.5.1　测试通过后，机构提交上线申请及各类配套材料。平台多部门联合评审，审核达标方可上线；未通过需整改补件，重新评审。
8.1.5.2　上线前双方分别完成生产环境配置、密钥及权限开通，同步数据、部署系统并完成自检，确保各项参数、接口、风控与结算规则配置无误，运行正常。
8.1.5.3　上线采用灰度发布模式，先小范围试点试运行 72 h，全程监测运行、交易、风控等状态。试运行无误后逐步扩量至全量上线，保障整体平稳运行、风险可控。
8.1.5.4　全量上线后，双方建立 7×24h 联合运维机制，实时监测系统、交易、资金、风控等运行情况，快速处置各类异常与问题。同时常态化开展巡检优化、安全加固、风险排查及应急演练，保障系统高稳运行，严控故障、安全与合规资金风险。
8.1.5.5　上线全流程资料完整留存、长期可追溯审计，存档期限不少于　5　年。业务纳入平台统一管控，保障运营合规稳定。

8.2　接口协议

8.2.1　基础协议

8.2.1.1 系统接口统一采用 RESTful API 规范，基于 HTTP/HTTPS 传输，优先启用 TLS 1.3 及以上版本 HTTPS 加密，不应明文传输，兼顾对接兼容性与数据传输安全。
8.2.1.2 数据传输统一使用 JSON 格式与 UTF-8 编码，规范驼峰字段命名、数据类型、时间格式及空值规则，统一数据标准，避免解析异常，保障传输规范、兼容稳定。
8.2.1.3 接口请求遵循 RESTful 规范，按场景区分 GET、POST、PUT、DELETE 方法，敏感操作统一使用 POST，语义明确、标准统一。
8.2.1.4 接口路径统一采用规范格式，通过版本号实现接口迭代与兼容，路径简洁清晰、标准统一，便于对接、运维与扩展。

8.2.2 版本控制

8.2.2.1 接口采用路径版本化管理，各版本独立运行、并行兼容，支持迭代升级与平滑过渡，不影响现有业务。
8.2.2.2 接口迭代坚守向下兼容原则，新增功能及优化内容独立建新版本，旧版本逻辑、参数保持不变。
8.2.2.3 下线旧接口宜提前至少 6 个月发布公告并提供迁移支持，过渡期正常维护，保障迁移平稳无风险。
8.2.2.4 版本变更全流程记录存档，保存时长不少于 5 年，满足审计、监管及追溯要求。
8.2.2.5 调用方建议优先使用最新版本，平台配套查询、测试与技术支持，助力平稳升级适配。

8.2.3 错误码要求

8.2.3.1 错误码分为系统级与业务级，编码唯一、分类清晰，方便问题定位与对接管理。明确系统级错误码含义，覆盖请求、认证、权限、接口、服务等各类通用异常场景、
8.2.3.2 统一业务级错误码定义，细分各类业务异常，精准定位交易、账户、风控等问题。错误码与提示信息固定绑定，新增异常宜分配独立编码，避免混乱与冲突。
8.2.3.3 错误码文档实时更新并对外开放，配套查询工具与技术支持，助力快速排障。

8.3 核心接口清单

8.3.1 钱包管理接口

钱包管理接口要求如下：

d) 对公钱包开户接口：核验资料与风控信息后完成开户，全流程校验留痕，安全合规；
e) 对公钱包销户接口：核查钱包状态与授权信息后办理注销，流程规范、全程审计；
f) 钱包充值接口：校验信息无误后完成资金划转，具备幂等、风控、对账等能力；
g) 钱包提现接口：核验余额与权限后办理提现，支持异常回滚，保障资金与账目准确；
h) B2B 转账接口：完成多方校验后执行企业钱包资金划转，适配企业资金调拨场景；
i) 资金归集接口：按规则将子钱包资金汇总至主钱包，支持多种归集模式，风控可追溯；
j) 钱包余额查询接口：校验权限后返回余额数据，响应快速，数据实时准确；
k) 交易明细查询接口：分页返回流水信息，支持导出与审计，数据长期留存。

8.3.2 支付结算接口

支付结算接口要求如下：

a) 主扫支付：用户扫码支付接口，支持 DO 到账、异步回调、退款、撤销、对账，适配线上 H5、线下静态码支付，保障支付快捷、安全、合规；
b) 被扫支付：商户扫码收款接口，适配商超、餐饮、售卖机等线下收银场景；
c) 批量转账：批量代发/批量结算接口，支持模板导入、异步处理、失败重发、对账、风控批量监控，适配薪资、补贴、货款批量结算，提升效率、降低人工风险；
d) 订单同步：订单状态同步接口，支持实时对账、异常排查、状态一致性校验、日志记录，保障商户订单与平台数据一致，避免单边账、长短款；
e) 支付结果回传：支付结果异步回调接口，确保回调可靠、不丢、不重，商户接收后校验、更新订单、触发履约，适配电商、线下、营销场景；

f) 退款申请：全额/部分退款接口，支持 DO 退款、异步回调、对账、风控拦截、日志审计，保障用户权益、商户合规。

8.3.3 智能合约类接口

为匹配能力服务层智能合约服务、资金监管模块自动化履约需求，增设智能合约专属接口，支撑自动化资金清算、多级分账等复杂利益分配场景，接口规范如下：

a) 合约部署接口：完成合约模板校验、参数配置、链上部署备案；
b) 分账比例配置接口：配置多方分账主体、分账比例、资金划转规则；
c) 合约状态查询接口：查询合约生效、执行、冻结、结清、终止全生命周期状态；
d) 合约自动执行接口：交易完成后自动触发分账、监管资金划转、履约扣款，内置幂等、回滚、风控拦截能力；
e) 合约注销接口：核验资金结清、无在途履约业务后注销合约。

8.3.4 接入管理接口

接入管理接口要求如下：

a) 机构注册：2.5 层机构注册接口，支持材料上传、格式校验、日志留痕、初审分流，作为接入唯一入口；
b) 资质提交：上传各类资质证件并提交审核，平台核验材料合规性与有效性，文件支持多格式上传，采用加密存储、脱敏展示并做版本管理，审核状态实时同步，资质全程可追溯；
c) 审核结果查询：提交机构 ID 与申请类型即可查询审核状态，平台返回结果、驳回原因及相关信息，支持实时查询、消息通知与日志留存，方便机构跟进进度、补正材料；
d) 接口权限申请：提交机构信息、权限清单及用途申请接口权限，平台结合风控与合规要求审批，遵循最小授权原则，配置有效期、限流及审计规则；
e) 联调测试：提交相关信息开展接口多项测试，平台反馈结果、日志与报错，配套沙箱、报告及复测记录，全面排查各类缺陷，保障上线质量；
f) 上线申请：提交各类上线材料后由平台联合评审，审核通过即开通生产权限、配发正式密钥并完成环境切换。配套灰度发布、实时监控与应急预案。

8.4 接口安全

8.4.1 身份认证

定期开展身份安全专项审计，每季度对机构Appid、访问密钥、系统账号、接口权限、IP白名单等关键配置进行全面复核，及时排查并修复身份认证流程中存在的漏洞、权限配置隐患及薄弱环节。

8.4.2 签名校验

8.4.2.1 所有接口请求与响应数据传输环节，采用国密 SM2/SM3 算法生成唯一数字签名，签名内容应包含 pp_id、req_id、timestamp 及数据摘要等关键要素，从技术层面保障接口数据传输的完整性、真实性、不可抵赖性。

8.4.2.2 签名密钥由平台与接入机构双方独立保管、分级存储，密钥从生成、分发、使用、存储到销毁的全流程均需全程留痕、可追溯，严防密钥泄露、滥用、丢失等风险。

8.4.2.3 平台在接收接口请求后，实时对请求签名进行三重校验，不应非法请求绕过安全机制。

8.4.2.4 签名算法统一采用国家认可的国密标准算法，不应使用弱算法、非标准算法；接口文档应明确签名规则、拼接顺序、编码格式及完整示例，接入机构应遵循标准执行，不应擅自修改算法或规则。

8.4.2.5 签名校验相关日志应采用加密方式长期留存，日志内容宜包含签名时间、算法类型、校验结果、异常原因等关键信息，支持审计追溯、风险排查、问题定位及纠纷处理，确保签名安全全程可追溯、可核查。

8.4.3 防重放

8.4.3.1 请求应携带唯一 req_id 和 5min 内有效的时间戳，平台校验拦截重复、超时请求，防范重放攻击。高敏感交易接口额外增加单次有效的随机 nonce，强化防重放能力，杜绝恶意重复交易。

8.4.3.2 超时请求直接拒绝，抵御延迟重放攻击，保障交易安全合规。防重放机制联动风控，针对异常高频请求执行限流、熔断、封禁等处置。

8.4.4 限流熔断

8.4.4.1 平台建立分级限流管控体系，按接入机构、接口类型、访问 IP 三个维度设置差异化调用频次、并发量、日调用总量限制，有效防范高频调用、恶意刷接口、流量耗尽等问题。
8.4.4.2 限流熔断规则支持动态配置、分级管控，核心支付、转账类接口设置限流阈值、更低的熔断触发条件，查询类接口适度放宽限制，兼顾系统安全性与业务可用性，适配不同场景需求。
8.4.4.3 限流熔断状态需实时可视化监控、自动告警通知，接入机构调用超限或触发熔断时，第一时间通过短信、平台消息等方式收到通知，支持快速调整调用频率、排查问题、恢复正常接入，降低业务影响。

8.4.5 权限管控

8.4.5.1 接口权限遵循最小必要、按需分配、分级管控核心原则，仅开放接入机构业务必需的接口权限，从源头避免权限滥用、越权调用、违规操作风险。
8.4.5.2 权限实行有效期管理、定期复核、自动回收机制，临时权限到期自动失效，长期权限每季度全面复核，及时清理闲置、过期、无效权限。
8.4.5.3 权限变更、新增、回收全流程应审批、全程留痕、可追溯，详细记录变更人、变更时间、变更原因、权限范围，支持审计核查、责任追溯、风险排查，确保权限管理合规可控。
8.4.5.4 系统实时拦截越权调用、违规访问行为，同步记录日志、触发告警、标记风险，必要时采取账号封禁、权限冻结等措施，快速处置违规调用，保障接口权限安全、合规、可控。

8.5 日志审计

8.5.1 日志采集

8.5.1.1 接口全链路操作日志应完整采集、无遗漏、无缺失，覆盖请求发起、响应返回等全环节，确保接口操作全程可追溯、可核查。
8.5.1.2 日志字段采用标准化、结构化设计，便于日志检索、统计分析、问题定位。
8.5.1.3 日志采集采用异步、非阻塞技术，不占用业务核心资源、不影响接口响应速度，确保日志采集不干扰正常业务运行，保障系统性能稳定。

8.5.2 日志存储

8.5.2.1 接口日志采用加密存储、多副本备份、异地容灾三重防护机制，确保日志数据安全可靠、可长期留存。
8.5.2.2 日志留存期限应遵循监管要求，满足监管追溯、审计核查、纠纷处理、风险复盘、合规检查等全周期需求。
8.5.2.3 定期清理过期日志、优化存储结构、清理冗余数据、提升查询性能，避免日志堆积、查询缓慢、存储溢出，保障日志存储高效稳定。
8.5.2.4 日志存储权限应管控、专人管理、加密访问，仅授权人员可查询、导出、分析日志，不应日志泄露、滥用、篡改，保障日志安全可控。

8.5.3 日志分析

8.5.3.1 日志实时分析、智能预警，自动识别异常调用、高频请求、错误激增、超时异常等安全风险，及时预警处置，防范安全事件。
8.5.3.2 支持多维度日志检索、统计分析、可视化展示，可按接入机构、接口类型、访问时间等维度筛选分析，快速定位问题、排查故障、优化策略。
8.5.3.3 日志分析与风控系统深度联动，识别风险后自动触发告警、限流、熔断、封禁等处置措施。定期开展日志审计、风险复盘，总结攻击特征、优化拦截策略、完善风控规则，持续提升安全防护能力，应对新型攻击手段。

8.5.4 审计追溯

8.5.4.1 接口操作全程可追溯、可审计，支持全链路追踪、还原操作现场，明确责任主体。
8.5.4.2 定期开展专项审计，核查接口合规性、安全性、权限合理性、日志完整性，及时发现并整改合规问题、安全隐患，保障接入活动合规可控。

8.5.5 异常处置

8.5.5.1 日志监控发现异常后，立即触发告警机制，通过短信、邮件、平台消息等方式同步通知管理员与接入机构，确保快速响应、及时处置。
8.5.5.2 异常分级分类处置，轻微异常预警提醒、跟踪观察，严重异常自动触发限流、熔断、临时封禁，重大异常立即启动应急预案，降低风险影响。
8.5.5.3 快速排查异常原因、定位问题根源、修复漏洞隐患、恢复正常服务，同步记录处置过程、结果、复盘总结，避免同类问题重复发生。
8.5.5.4 定期开展异常复盘、总结经验、优化规则、完善预案，持续提升异常识别、处置能力，保障接口长期安全稳定运行。

9 运营管理要求

9.1 资质管理

9.1.1 准入资质

9.1.1.1 2.5 层金融机构接入具备合法有效的营业执照、金融许可证或支付牌照等法定资质，确保接入主体合法合规、具备金融服务资质。
9.1.1.2 接入机构应具备独立、完善的技术系统、专业风控团队、合规管理体系及专业运维能力，满足数字人民币业务运营、风控、合规、运维全流程要求。
9.1.1.3 接入机构应与平台签署正式合作协议、保密协议、合规承诺书，明确双方权责、风险责任、合规义务，保障合作合规、权责清晰、风险可控。

9.1.2 资质核验

9.1.2.1 建立年度资质核验机制，每年对 2.5 层金融机构资质有效性、状态、变更情况进行全面核查，及时更新过期资质、纠正资质异常。
9.1.2.2 接入机构发生法人、名称、地址、资质等变更时，主动向平台报备并提交更新材料，确保资质信息与实际一致、同步更新。
9.1.2.3 资质核验全流程留痕、归档留存，详细记录核验时间、结果、材料、整改情况，支持审计追溯、合规核查、责任追溯。
9.1.2.4 资质核验结果与风控系统联动，资质异常自动触发预警、暂停业务、核查处置，保障接入活动合规可控。

9.2 人员管理

9.2.1 岗位设置

9.2.1.1 接入机构应设立系统运维、接口管理、数据管理、风控监控、合规审核、客户服务等专职岗位，分工明确、权责清晰、各司其职，保障业务全流程有序开展。
9.2.1.2 关键岗位实行双人双岗、相互制衡机制，杜绝单人操作、单人决策风险，防范权限滥用、违规操作。
9.2.1.3 宜建立关键岗位轮岗机制，轮岗周期根据机构规模与岗位风险合理确定。
9.2.1.4 制定标准化岗位职责、操作规范、权限边界、责任追究机制，文档化、制度化管理，确保岗位工作有章可循、规范开展。
9.2.1.5 岗位人员应具备金融与 IT 复合专业背景，持证上岗、专业匹配，保障岗位履职能力。

9.2.2 人员资质

9.2.2.1 从业人员需通过数字人民币专项培训、考核合格后方可上岗，熟悉数字人民币业务规则、技术规范、监管要求，具备专业履职能力。

9.2.2.2 从业人员需熟练掌握数字人民币业务、接口操作、风控规则、合规要求，熟悉相关法律法规、监管政策，保障业务合规开展。
9.2.2.3 从业人员应具备网络安全、数据安全、反洗钱等专业能力，通过相关认证，具备风险识别、处置能力。
9.2.2.4 建立年度继续教育机制，每年开展不少于 2 次专业培训，更新知识、提升技能、强化合规意识，适配业务发展需求。
9.2.2.5 从业人员宜通过背景审查，无不良从业记录、违法违规记录，确保人员可靠、合规、廉洁。

9.3 风控管理

9.3.1 交易风控

9.3.1.1 实时监控大额、高频、异地、异常交易，设置分级预警阈值，自动识别并拦截可疑交易，防范洗钱、诈骗、套现风险。
9.3.1.2 精准识别洗钱、诈骗、非法集资、可疑交易特征，实时上报、冻结可疑资金、阻断风险扩散，保障资金安全。
9.3.1.3 建立交易限额管控体系，设置个人、企业单笔、日、月交易限额，超限额自动拦截、人工复核，防范大额风险。
9.3.1.4 建立交易黑白名单机制，拉黑高风险商户、用户，不应交易，精准防控风险主体。
9.3.1.5 实行交易全链路风控，覆盖事前预警、事中监控、事后追溯，全流程防控交易风险。

9.3.2 接口风控

9.3.2.1 实时监控异常调用、高频攻击、越权访问、参数篡改、恶意刷接口行为，自动拦截、告警处置，防范接口安全风险。
9.3.2.2 实行接口限流熔断、异常降级机制，异常时快速降级、阻断故障扩散，维护核心系统稳定。
9.3.2.3 定期开展接口调用日志审计，识别攻击特征、优化风控规则、提升防护能力。
9.3.2.4 建立接口黑白名单，拉黑高风险 IP、异常机构，不应接入，精准防控接入风险。
9.3.2.5 接口风控与系统深度联动，异常自动触发限流、封禁，快速处置风险。

9.3.3 资金风控

9.3.3.1 实时监控资金流向、归集、分账、冻结、解冻等全流程，识别资金异常、违规流转、挪用风险，及时预警。
9.3.3.2 实行专款专用、专户监管机制，确保监管资金、专项资金定向使用、不被挪用、合规支出。
9.3.3.3 建立资金对账风控机制，实时核对资金流水、余额，发现差异立即核查、闭环处理。
9.3.3.4 大额资金划转实行双人复核、风控审批机制，严控大额资金风险、防范违规操作。
9.3.3.5 资金异常时快速冻结、处置、溯源，保障资金安全、风险可控。

9.4 对账管理

9.4.1 日对账

9.4.1.1 实行 D0 实时对账+T+0 日终对账双机制，每日逐笔核对交易笔数、金额、流水、状态，确保账实一致；对账覆盖钱包、支付、转账、退款、归集、营销等全业务场景，无遗漏、无死角。
9.4.1.2 对账差异当日排查、闭环处理，不隔夜、不挂账，及时解决单边账、长短款等问题；对账以自动化为主、人工复核为辅，提升对账效率、降低人工差错。

9.4.2 对账差异

9.4.2.1 将对账差异分类为单边账、长短款、状态异常、数据延迟，差异化处置、精准解决。单边账快速定位、冲正补录、留痕追溯，确保数据一致、账实相符。
9.4.2.2 长短款核查原因、追回资金或赔付损失、追责问责，防范资金损失。差异处理全流程审批、双人复核、留痕可追溯；定期复盘差异原因、优化流程、减少差异发生，提升对账质量。

10 应急处置

10.1 应急预案

10.1.1 预案宜覆盖系统宕机、网络中断等各类风险场景，全面防控；明确预警、响应、止损、排查、恢复、复盘全流程，职责清晰、流程规范。

10.1.2 宜分级应急预案体系，按事件影响范围、业务中断时长、资金损失规模、数据泄露量级、舆情风险划分为一级（特别重大）、二级（重大）、三级（一般）三级应急预案分级判定标准如下；

a) 一级（特别重大）应急响应：
   1) 数字人民币核心交易系统全域瘫痪、跨区域业务完全中断、批量核心敏感数据泄露、大额资金被盗/挪用、遭受国家级持续性网络攻击、引发大规模舆情；
   2) 全部渠道无法办理收付、钱包开户、资金监管业务，预计中断时长超 4 h。
b) 二级（重大）应急响应：
   1) 局部区域/核心子系统故障、50%以上线上、线下渠道交易受阻、少量敏感数据外泄、单笔大额资金异常流转、持续性网络攻击导致业务严重降级；
   2) 业务中断预估 1～4 h，仅局部渠道可维持基础查询。
c) 三级（一般）应急响应：单条接入链路、单一非核心功能、局部终端故障，仅少量用户交易受影响，无数据泄露、无大额资金风险，业务中断预估 1 h 以内。

10.1.3 2.5 层金融机构应针对数字人民币钱包、支付结算、资金监管、智能合约等核心交易系统设定刚性容灾指标，形成业务连续性方案并落地灾备架构；

a) RTO（恢复时间目标）：
   1) 核心交易系统（收付、转账、监管资金）：RTO≤15 min；
   2) 商户进件、营销、报表等非核心业务系统：RTO≤2 h；
   3) 村镇银行、小型支付机构等轻量化主体，核心系统 RTO 最长不得超过 30 min。
b) RPO（恢复点目标）：
   1) 核心交易数据、钱包资金流水：RPO≤5 min，采用实时同步复制；
   2) 商户、营销、日志类业务数据：RPO≤30 min；
   3) 所有 RTO/RPO 指标每年结合业务规模、交易峰值重新评估调整，留存评估报告备查。

10.2 处置流程

10.2.1 监控发现异常后立即预警、快速上报、启动响应，第一时间掌握情况，分级启动应急预案、成立应急小组、明确分工、协同处置，高效应对。

10.2.2 快速止损、冻结资金、隔离风险、阻断故障扩散，降低损失，精准排查、定位问题、修复故障、恢复服务，快速恢复业务；复盘总结、优化流程、完善预案、避免同类问题重复发生。

10.3 应急演练管理

10.3.1 演练频次

演练频次要求如下：

a) 三级、二级应急场景综合演练：每半年至少开展 1 次；
b) 一级重大灾难场景专项演练：每年至少开展 1 次；
c) 接入链路切换、数据库主备切换、接口熔断等单点故障实操演练：每季度至少于 1 次；
d) 村镇银行、小型支付机构可合并简化演练，但全年演练总场次不得少于 3 次。

10.3.2 演练管理要求

演练覆盖故障模拟、分级响应、灾备切换、止损操作、监管报送全流程，演练后形成评估报告，校验RTO/RPO指标是否达标，未达标项限期整改闭环，演练记录、视频、报告等归档审计。

10.4 监管报送要求

10.4.1 报送时限

监管报送时限如下：

a) 事发后 1 h 内向属地人民银行分支机构、运营机构提交简要快报，说明事件类型、影响范围、初步处置措施；
a) 事件处置全过程每 2 h 报送进展更新，处置完成后 24 h 内提交完整事件专项报告；
b) 全部处置结束后 10 个工作日内提交深度复盘调查报告；
c) 三级一般故障仅内部留存记录，无需即时监管报送，但年度应急评估时统一汇总上报。

10.4.2 报送内容

快报及正式报告需包含机构信息、事件等级、故障起止时间、受影响用户/商户规模、资金风险情况、处置措施、数据泄露范围、整改计划等关键内容，所有报送记录加密存档，满足监管追溯检查要求。